IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Patent Application

Applicant(s):	Philip D. MacKenzie
Case:	15
Serial No.:	10/600,687
Filing Date:	June 20, 2003
Group:	2435
Examiner:	Baotran N. To
Title:	Methods and Apparatus for Providing Secure Two-Party Public Key Cryptosystem

REPLY BRIEF

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313

Sir:

The remarks which follow are submitted in response to the Examiner's Answer dated January 21, 2010, in the above-identified application. The arguments presented by Appellant in the corresponding Appeal Brief are hereby incorporated by reference herein.

In Section 10 of the Answer, on pages 11-17, the Examiner responds to various arguments raised by Appellant in the Appeal Brief.

REMARKS

I. Claims 1, 8, 9 and 16 (pages 11-15 of the Answer)

The Examiner continues to assert that the limitation wherein the first party device and the second party device jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds, is disclosed by Faucher at column 8, lines 8-55 and Fig. 5. Appellant strongly disagrees with this assertion.

The Examiner argues on page 13 of the Answer that "Appellant has failed to explicitly identify the specific claim limitation 'the joint decryption operation' that would define a patentable distinction over prior art. Appellant merely mentions 'the joint decryption operation' in the claim, but does not define metes and bounds of the term 'joint decryption operation.'"

Appellant respectfully disagrees. The recitation of "the joint decryption operation" clearly refers back to the recitation, found within the same limitation of the claims, of a decryption operation jointly performed by the first party device and the second party device. Moreover, the claim itself states that the recited joint decryption operation is performed by the first party device and the second party device each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds.

The Examiner further contends on page 14 of the Answer that "the features upon which applicant relies (i.e., each perform one or more subcomputations of the singular decryption operation) are not recited in the rejected claim(s)." (emphasis in original) Appellant respectfully disagrees. The claims at issue each recite "a decryption operation" (note the use of singular rather than plural) jointly performed by the first party device and the second party device.

Again, the claim language clearly provides for a jointly performed decryption operation of a given ciphertext. That is, as made clear by the claim language, the first party and the second party each perform one or more subcomputations of the decryption operation that results in the decryption of the given ciphertext, and that such subcomputations are based at least in part respective partial shares of a key that each party holds. Thus, neither party can decrypt the given ciphertext alone. This is what is meant by a joint decryption operation.

On pages 12-13 of the Answer, the Examiner argues that Faucher discloses such a joint decryption operation in column 8, lines 25-48. While there is information exchanged between the two Faucher terminals and decryptions are performed, no where do the two Faucher terminals "jointly perform a decryption operation of the ciphertext by each respectively performing one or more subcomputations of the joint decryption operation based at least in part on respective partial shares of a key that each party holds," as recited in the independent claims. In fact, the entire protocol of column 8 of Faucher is performed in order to generate a session key, which is done by each terminal performing separate decryption operations of certificates received from the other terminal. See Faucher at column 8, lines 38-54.

There is no joint performance of a joint decryption operation of a ciphertext whereby each terminal performs subcomputations of the joint decryption operation. Nor is there any disclosure in Faucher that suggests that any such subcomputations are based at least in part respective partial shares of a key that each party holds. In fact, column 8, lines 25-28, of Faucher confirms this deficiency by clearly explaining that each terminal independently decrypts the other's certificate using the KCA public decryption key: "Terminal A decrypts and validates terminal B's certificates using the KCA public decryption key. Similarly, terminal B decrypts and validates terminal A's certificate using the KCA public decryption key."

Again, Faucher clearly does not disclose that the first party and the second party each perform one or more subcomputations of the singular decryption operation that results in the decryption of the given ciphertext, and that such subcomputations are based at least in part respective partial shares of a key that each party holds. The operations between the first and second parties in Faucher are performed to generate a session key so that each party can be authenticated to the other for any subsequent transfers, not to jointly decrypt the ciphertext.

Cramer fails to remedy theses deficiencies of Faucher. Accordingly, it is believed that the combined teachings of Cramer and Faucher fail to meet the limitations of claim 1.

With regard to the last paragraph of page 14 of the Answer, Appellant respectfully maintains that the Examiner has still failed to identify a cogent motivation for combining Cramer and Faucher in the manner proposed. Rather, the Examiner has merely provided further conclusory statements of the sort rejected by both the Federal Circuit and the U.S. Supreme Court. See *KSR Int'l Co. v.*

Teleflex Inc., 127 SCt 1727, 1741, 82 USPQ2d 1385, 1396 (U.S. 2007), quoting *In re Kahn*, 441 F. 3d 977, 988 (Fed. Cir. 2006) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness."). Appellant further notes that "knowledge of a problem and motivation to solve it are entirely different from motivation to combine particular references to reach the particular claimed method." *Innogenetics N.V. v. Abbott Laboratories*, 512 F3d 1363, 85 USPQ2d 1641, 1648 (Fed. Cir. 2008)

For at least these reasons, Appellant asserts that claim 1 is patentable over Cramer and Faucher.

Independent claim 8, 9 and 16 include limitations similar to those of claim 1, and is therefore believed allowable for reasons similar to those described above with reference to claim 1.

<u>II. Claims 2 and 10</u> (pages 15-16 of the Answer)

In addition to being allowable for at least the reasons identified above with regard to claims 1 and 9, claims 2 and 10 are also believed to define separately-patentable subject matter over the cited art. More particularly, claims 2 and 10 recite an exchange of information between the first party device and the second party device whereby at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using <u>its own public key</u> and <u>another party can not read the information</u> but can use the information to perform an operation.

The Examiner refers to Faucher at column 8, lines 8-55, as disclosing this limitation. Appellant notes that this is the <u>very same portion of Faucher</u> which the Examiner has argued "explicitly discloses the decryption operation" on page 11 of the Answer.

Indeed, Faucher discloses a technique in which "Terminal B calculates the corresponding public component X^{R_b} mod P, encrypts it using the public encryption key PK_a extracted from terminal A's certificate and transmits $PK_a(X^{R_b} \bmod P)$ to terminal A. Terminal A receives and decrypts the message [and] obtains Terminal B's public random component X^{R_b} mod P. . . ." See Faucher at column 8, lines 34-40.

In other words, Faucher discloses a technique in which Terminal B encrypts its public random component X^{R_b} mod P <u>using Terminal A's public encryption key</u> (PK_a), and in which

Terminal A decrypts the message and obtains Terminal B's public random component $X^{R_b} \bmod P$). This is clearly different from the technique recited in claims 2 and 10 in which at least a portion of the information is encrypted using an encryption technique such that one party encrypts information using its own public key and another party can not read the information but can use the information to perform an operation. Thus, Faucher fails to remedy the deficiencies of Cramer with regard to the limitations of claims 2 and 10.

III. Claims 4 and 12 (page 16 of the Answer)

In addition to being allowable for at least the reasons identified above with regard to claims 1 and 9, dependent claims 4 and 12 are also believed to define separately-patentable subject matter over the cited art. More particularly, claims 4 and 12 recite generating a share of a random secret; generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext; transmitting at least the encrypted information to the second party device; and computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

The Examiner again refers to Cramer at column 7, lines 11-19 as teaching or suggesting the step of generating a share of a random secret. The relied-upon portion of Cramer refers to a private-key choosing step, and does not teach or suggest generating a share of a random secret. Although Cramer, at column 7, lines 10-27 refers to private key Z_q, the relied-upon portions of Cramer do not teach or suggest generating information representing encryptions of a form of the random secret, a share of a private key, and the ciphertext. Furthermore, although Cramer at column 9, lines 25-50 refers to recovering the plaintext m in the decryption step 50, Cramer does not teach or suggest computing the plaintext based at least on the share of the random secret, the share of the private key, the ciphertext, and the data received from the second party device.

Claims 5 and 13 (not addressed in the Answer)

In addition to being allowable for at least the reasons identified above with regard to claims 1 and 9, dependent claims 5 and 13 are also believed to define separately-patentable subject matter over the cited art. More particularly, claims 5 and 13 include limitations wherein the first party device and the second party device additively share components of a private key.

The Examiner refers to Cramer at column 7, lines 10-15 and column 9, lines 35-40 as teaching or suggesting the limitations of claims 5 and 13. However, the relied-upon portions of Cramer do not teach or suggest the recited limitations. Column 7, lines 10-15 of Cramer refers to private-key choosing step 13, and column 9, lines 35-40 refer to decryption of an encryption of a message, which do not teach or suggest the first party device and the second party device additively sharing components of a private key.

IV. Claims 6 and 14 (pages 16-17 of the Answer)

In addition to being allowable for at least the reasons identified above with regard to claims 1 and 9, dependent claims 6 and 14 are also believed to define separately-patentable subject matter over the cited art. More particularly, claims 6 and 14 include limitations directed to generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

The Examiner again refers to Cramer at column 8, line 38 through column 9, line 23, as teaching or suggesting the limitations of claims 6 and 14. However, the relied-upon portion of Cramer refers to verification of ciphertext 30 in verification step 40, which fails to teach or suggest generation and exchange of proofs between the first party device and the second party device that serve to verify operations performed by each party.

V. Claims 3, 7, 11 and 15 (page 17 of the Answer)

Appellant respectfully maintains that the Cramer paper reference fails to remedy the deficiencies described above with regard to Cramer and Faucher. Thus, claims 3, 7, 11 and 15 are patentable at least by virtue of their dependency from claims 1 and 9.

In view of the above, Appellant respectfully maintains that claims 1-16 are in condition for allowance, and respectfully request reversal of the §103(a) rejections.

Respectfully submitted,

Date: March 22, 2010

David E. Shifren
Attorney for Appellant(s)
Reg. No. 59,329
Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2641